Thank you for your comment, Robert Bea.

The comment tracking number that has been assigned to your comment is POCSWS50029.

Comment Date: March 16, 2016 11:26:29AM
Well Stimulation Treatments on the Southern California OCS Draft EA
Comment ID: POCSWS50029

First Name: Robert
Middle Initial: G
Last Name: Bea
Organization: Center for Catastrophic Risk Management, College o
Address: 60 Shuey Drive
Address 2:
Address 3:
City: Moraga
State: CA
Zip: 94556
Country: USA
Privacy Preference: Don't withhold name or address from public record
Attachment: SRAM + uncertainties2 - CCRM.pdf

Comment Submitted:

BOEM has not performed a comprehensive environmental Risk Assessment (RA) based on the established principles of System Risk Assessment and Management (SRAM); reference attachment. such a RA must be performed before the proposed OCS activities are approved.

UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

TELEPHONE: (925) 631 1587

E-MAIL: bea@ce.berkeley.edu

CENTER FOR CATASTROPHIC RISK MANAGEMENT
DEPARTMENT OF CIVIL & ENVIRONMENTAL ENGINEERING
BERKELEY, CALIFORNIA 94720-1710

System Risk Assessment and Management

The universal goal of System Risk Assessment and Management (SRAM) is to anticipate, prevent, control, and mitigate major accidents involving complex, engineered, human-based systems.

SRAM practices, codes, and regulations were driven initially by several catastrophic accidents that occurred during the 1950s and 1960s and by development of new high-risk systems such as those associated with commercial nuclear power generation, jet powered aviation, and chemical refining. In the field of chemical refining, SRAM is known as "Process Safety."

SRAM is distinct from the concept of personal safety, which is sometimes referred to as "workplace safety" or "occupational health and safety." Personal safety focuses on the prevention of workplace injuries and harm to people through things such as slips, trips, and falls. On the other hand, SRAM focuses on major hazards impacting safety, environmental damage and business losses.[1] Personal safety is a subset of SRAM; they represent different challenges in developing the acceptable performance of engineered systems.

SRAM begins with the identification and assessment of risks within an 'Engineered System.' Experience clearly indicates that in order to effectively develop and implement SRAM processes, an organization must address this challenge by properly characterizing and analyzing its Engineered Systems. In some cases, there are important performance interactions that are developed by multiple Engineered Systems whose combined effects are different from and often greater than associated with the individual Engineered Systems.

An Engineered System can be characterized as consisting of seven interconnected, interdependent, interactive components:

- **Operating teams** - people that have direct contacts with and responsibilities for the design, construction, operation, maintenance, and decommissioning of the system;
- **Organizations** - groups that influence how the operating personnel conduct their operations and provide the resources, means, methods, and incentives for the conduct of these operations;
- **Procedures** - formal and informal, written and unwritten, and digital computer practices and programs that are used in performing operations;
- **Hardware** - with which the operations are performed;
- **Structure** – constructed assemblies that provide supports and containments required for system operations;
- **Environments** - external, internal, and social, and
- **Interfaces** among the foregoing.

[1] *Guidelines for Preventing Human Error in Process Safety*, Center for Chemical Process Safety, New York, 1994; *see also* American Petroleum Institute, *available at* http://www.api.org/environment-health-and-safety/process-safety.

In-depth studies of past catastrophic accidents have demonstrated such failures involve malfunctions developed in and by all six components. This is a unique characteristic of Engineered System failures. Another unique characteristic is that the components that consistently make the largest contributions (typically more than 80 percent) to causation of Engineered System failures are the "people-based human" components involving Operating Teams, Organizations, and their Interfaces. Studies show the leading malfunctions involved in human components are those associated with organizational and operating team cultures, communications, and violations (intentional departures from required practices). For this reason, major system accidents and disasters frequently been identified as "Organizational Accidents."[2]

Risk is defined as the likelihoods and consequences associated with major accidents and disasters that involve Engineered Systems (Figure 1). ***Systems having higher potential consequences require lower likelihoods of failure*** in order to be deemed "Fit-For-Purpose."

The goal of SRAM during the life-cycle of an Engineered System is to manage, engineer, construct, operate, and maintain the system so it has acceptable performance and quality characteristics. An Engineered System is deemed to be 'Safe' when its risks have been successfully managed to be 'As Low As Reasonably Practicable' (ALARP).

Once potential hazards and threats to acceptable performance of an engineered system have been identified, they must be properly assessed. The assessment of a risk associated with a given Engineered System has two basic components: (1) determination of the likelihood of an engineered system developing an adverse event from a system failure or other disaster; and (2) determination of the potential adverse consequences associated with such an event.[3]

There are varying techniques for determining the likelihoods and consequences of an adverse event. The primary techniques for evaluation include:

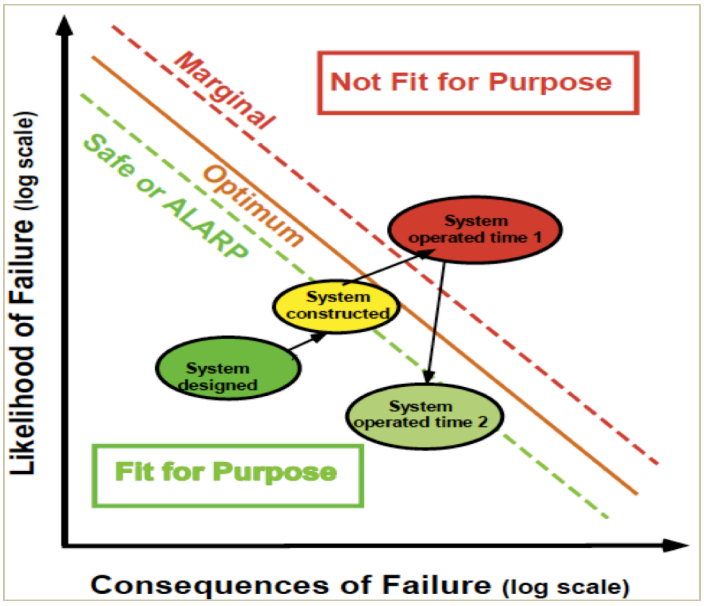

Figure 1: System risk assement and management

- **Qualitative** (non-numeric, subjective, generally consisting of a high, medium, low-type assessments);
- **Quantitative** (numerical, objective, mathematical measurement of risk as in a Quantified Risk Assessment - QRA or a Probabilistic Risk Assessment - PRA); and
- **Mixed** (combination of qualitative and quantitative).

As the probabilities and potential adverse consequences associated with an Engineered System become very large, a mixture of qualitative and quantitative factors and methods are used to develop the quantitative values of the likelihoods and consequences used in SRAM. Although there are varying techniques for evaluating the likelihood and consequences of a failure, results from each technique must meet one essential requirement: they must be *verifiable and verified*. The analyses must be performed by people having the *requisite qualifications of knowledge and experience* to perform such assessments.

---

[2] *Managing the Risks of Organizational Accidents*, James Reason, Ashgate Publishing Co., Brookfield, VT

[3] *Guidelines for Chemical Process Quantitative Risk Analysis*, Center for Chemical Process Safety, New York, 1989; *Fundamentals of Risk Analysis and Risk Management*, Vlasta Molak, CRC Lewis Pubishers, New York, 1997; *Human & Organizational Factors: Risk Assessment & Management of Engineered Systems*, Robert Bea, Vick Copy Publishers, Berkeley, CA, 2009.

Further, the analyses must be performed so as to 'neutralize' a wide variety of potential 'biases' that can exert important influences on the results (e.g. wishful thinking, conformational bias). These biases often result in dramatic under-estimates in both the likelihoods and consequences of major failures that lead to false senses of Safety. A risk evaluation that is not properly qualified and validated (externally and internally) can undermine SRAM processes. The primary reason for performing qualified evaluation processes for 'high-risk' engineered systems is encapsulated by the SRAM theme: "***one can not properly manage what one can not properly measure."***

Additionally, in conducting such a risk assessment, it is critical to understand that the variables associated with an event are conditional and dynamic – changing based upon "environmental" conditions and organization - operating decisions and actions. Organizational and operating decisions can greatly increase the accumulated risk level of an engineered system. This is particularly true if the linkage between prior decisions and subsequent decisions is not made (*i.e.*, if decisions are reached independently or "siloed" without full consideration of their overall potential impact on the performance and reliability of the engineered system). Accordingly, a proper SRAM will have procedures and policies in place that allow the Engineered System to, in certain cases, adjust or adapt to account for changed failure likelihood and consequence variables, and in other cases, cease operations of the Engineered System in order to allow implementation of processes to reduce the risk and/or consequence variables to Safe or ALARP levels.

Risks result from uncertainties. To provide organization and structure for classification, description, and analyses of the different types of uncertainties, they have been organized here into two fundamental categories 1) **Intrinsic** – belonging to the essential nature, and 2) **Extrinsic** – what comes from outside of something.

There are two types of Intrinsic uncertainties: Type 1 – natural, inherent, information (data) insensitive, and Type 2 – analytical modeling (qualitative and quantitative), parametric, state, information sensitive. Knowledge and data can be used effectively to reduce Type 2 uncertainties. Other means like Factors-of Safety can be used to cope with Type 1 uncertainties.

There are two types of Extrinsic uncertainties: Type 3 – human and organizational task performance; and Type 4 – human and organizational information development and utilization. Results from Extrinsic uncertainties frequently are identified as 'human errors.' Experience has amply demonstrated that such errors are results from human and organizational processes and are not the 'root causes' of accidents and failures. Human errors are results, not causes.

Type 4 uncertainties have been divided into two sub-categories: a) Unknown Knowables – "Predictable Surprises" or "Black Swans"[4], and b) Unknown Unknowables [5] – not predictable or knowable before something is done. In the case of Unknown Knowables, the knowledge exists but has not been properly accessed, analyzed, and understood. In the case of Unknown Unknowables, the knowledge does not exist and the uncertainties and their effects are not predictable. In this case, the knowledge must be developed at different times and ways during the life of a system, properly analyzed, and appropriate actions taken to understand these uncertainties to enable preservation of the operational integrity of a system. Recognition of and preparation for Unknown Unknowable uncertainties makes it clear that processes to understand and manage uncertainties performed before a system exists and is operated can and never will be complete. Developing safe and reliable systems is a continuing 'improvement' process to properly recognize and defend systems for ambiguities.

Some engineers do not think that Extrinsic uncertainties should be included in risk assessments. They contend that only Intrinsic uncertainties should be included. They rely on 'management processes' to properly

[4] Bazerman, M.H. and Watkins, M.D. (2004). *Predictable Surprises*, Harvard Business School Press, Boston, MA. Taleb, N.N. (2007). *The Black Swan*, Random House Publishing Group, New York, NY.

[5] Bea, R.G. (2002). "Human and Organizational Factors in Design and Operation of Deepwater Structures," Proceedings Offshore Technology Conference, Society of Petroleum Engineers, OTC 14293, Richardson, TX.

address Extrinsic uncertainties. This reliance potentially results in a dramatic under-estimate in the risks because typically the Extrinsic uncertainties account for 80% or more of the risks that developed when major failures or accidents are realized.

As shown in Figure 1, if an engineered system evolves or migrates into the Not-Fit-For-Purpose risk region, timely and effective management, engineering, and operations processes must be implemented to reduce the likelihood of failure (*e.g.* increase number of and robustness of prevention barriers) and consequences of failure (*e.g.* risk mitigations to reduce the impact of consequences, emergency planning, crisis management and response contingencies, personnel training and drills). An effective SRAM system reduces the risk of catastrophic failure and, among other things, allows an organization to bring its engineered systems back into the "Fit-For-Purpose," or ALARP risk region. SRAM guidelines require suspension of operations associated with a system that has been evaluated to be above the maximum tolerable ALARP risk level. A system is deemed "Safe" only when it is operated in the "Fit-For-Purpose" risk region.

How Safe is Safe Enough?

A key part of SRAM is a determination of what constitutes a tolerable level of risk (Figure 2).[6] This determination is intended to answer the key question: "how safe is safe enough?" The answer to this question defines in quantitative terms the primary goal of SRAM during the life-cycle of a given engineered system: to manage, engineer, construct, operate, and maintain the system so it has desirable performance, service, and reliability (i.e., Safety characteristics) with ALARP risks. Safety is defined formally as "freedom from undue exposure to injury or harm."

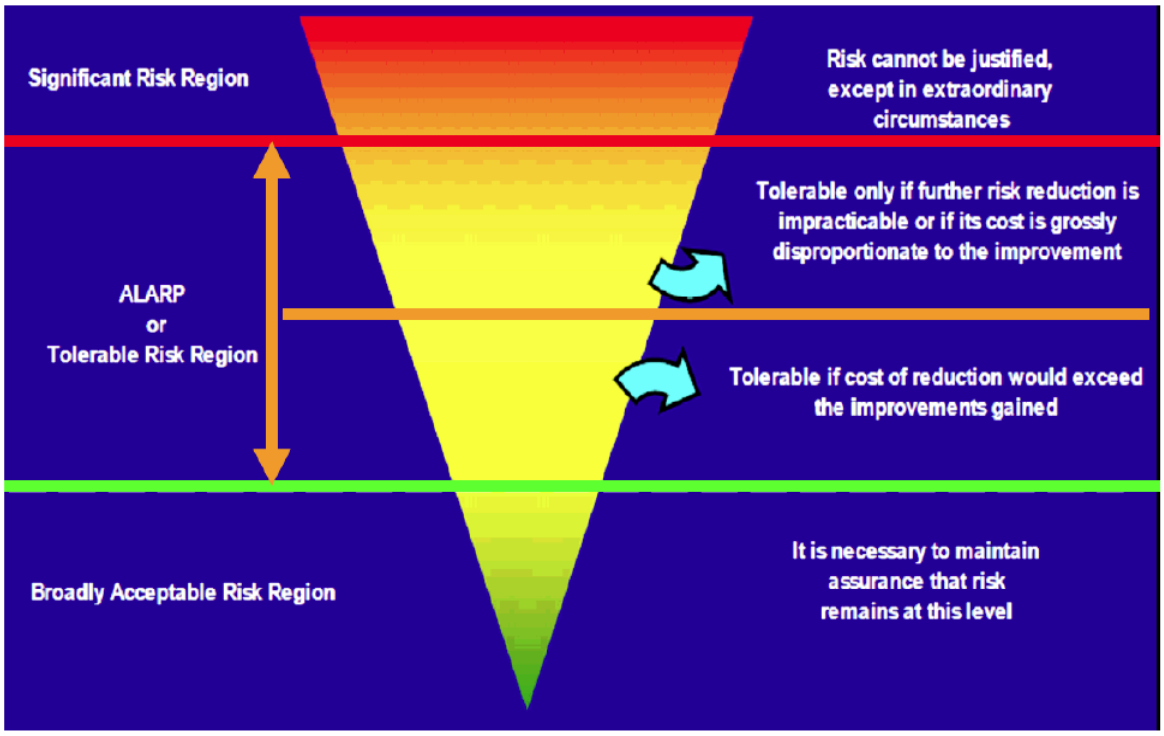

Figure 2: The SRAM ALARP Risk Region.

[6] Robert Bea, *Reliability Based Design Criteria for Coastal and Ocean Structures*, The Institution of Engineers, Australia, Barton ACT (1990); Edward Wenk, Jr, *"How Safe is Safe? Coping With Mother Nature, Human Nature, and Unintended Consequences,"* Working Paper, Deepwater Horizon Study Group, Berkeley, CA. 2010; Baruch Fischhoff, Sarah Lichtenstein, Paul Slovic, Stephen Derby, and Ralph Keeney, *Acceptable Risk*, Cambridge University Press, 1981.

The ALARP Risk Region is developed from a formal collaborative process involving industry (representing stockholder and commercial interests) and government (representing the general public and environmental interests).[7] Achieving and maintaining the agreed upon "tolerable" ALARP level of risk is the responsibility of the owner / operator of the engineered system; this is 'goal based' SRAM. The responsibility of government is to develop regulatory, legislative, and judicial processes to verify that the ALARP Risk responsibility has been met during the life of an Engineered System.

Three general approaches have been used to help define the ALARP region: Cost-Benefit economic analyses, Historic Precedents analyses, and Standards of Care (Standards of Practice) analyses.[8] Through Historic Precedents and Standards of Care decisions, the law serves as an important instrument to encourage acceptable assessment and management of system risks.

Risk Management

After a risk is identified and assessed, SRAM requires appropriate "barriers" be developed and maintained to prevent, control, and/or mitigate the consequences of major accident risks. Prevention and mitigation response barriers (Figure 3) include Proactive (performed before activities), Interactive (performed during activities), and Reactive (performed after activities) approaches to identify, manage, and control system failure likelihoods and consequences. Such barriers are intended to be fully integrated and implemented throughout the entire life (from concept development through decommissioning) of an engineered system.

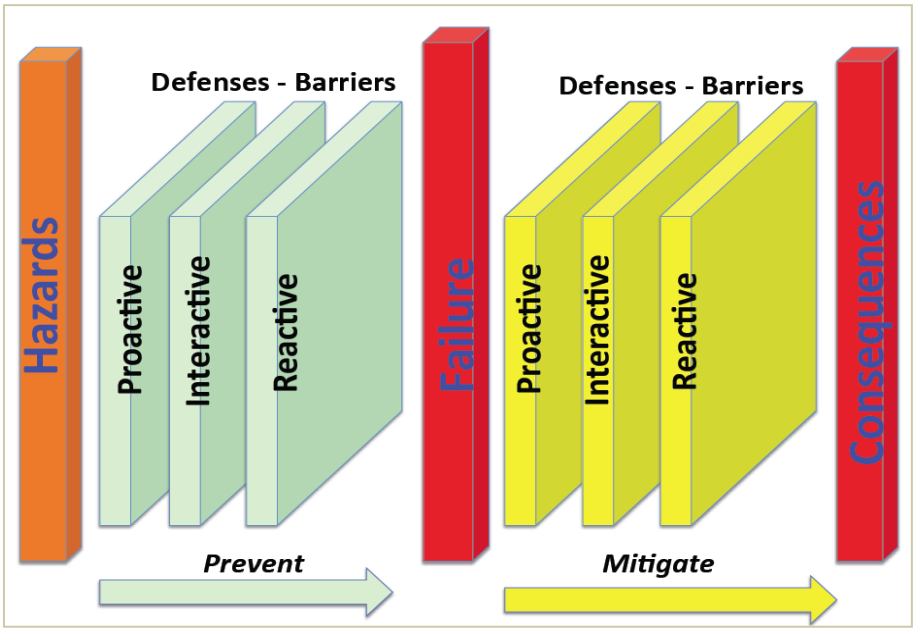

Figure 3: Failure prevention barriers and consequence mitigation barriers.

The role of PSM prevention and mitigation barriers during operations of an Engineered System is

[7] D.N.D. Hartford, Legal framework considerations in the development of risk acceptance criteria, Structural Safety, Vol. 31, 2009, Elsevier Publishers; Edward Wenk, Jr., How Safe is Safe? Coping with Mother Nature, Human Nature and Technology's Unintended Consequences, Center for Catastrophic Risk Management, Deepwater Horizon Study Group Working Paper, Jan. 2011, ref. http://ccrm.berkeley.edu/deepwaterhorizonstudygroup/dhsg_resources.shtml

[8] R. Bea, Quality Goals: Acceptable Reliability and Risk, Center for Catastrophic Risk Management, University of California Berkeley, 2003.

illustrated by the "Swiss Cheese Model" (Figure 4).[9] The barriers are intended to stop hazardous activities from developing disaster causation "spears" that can penetrate or defeat the prevention and mitigation barriers. The barrier "holes" (defects and deficiencies in SRAM) are created by "active activities," such as unsafe operator acts, and by "latent activities," such as defects embedded in the system during activities. Active holes are developed by the system "operators" who work at the "sharp end" of the disaster spear. Latent holes are developed by the system's responsible organization's "management" (commercial and regulatory) components distributed along the "shaft" (blunt end) of the disaster spear.

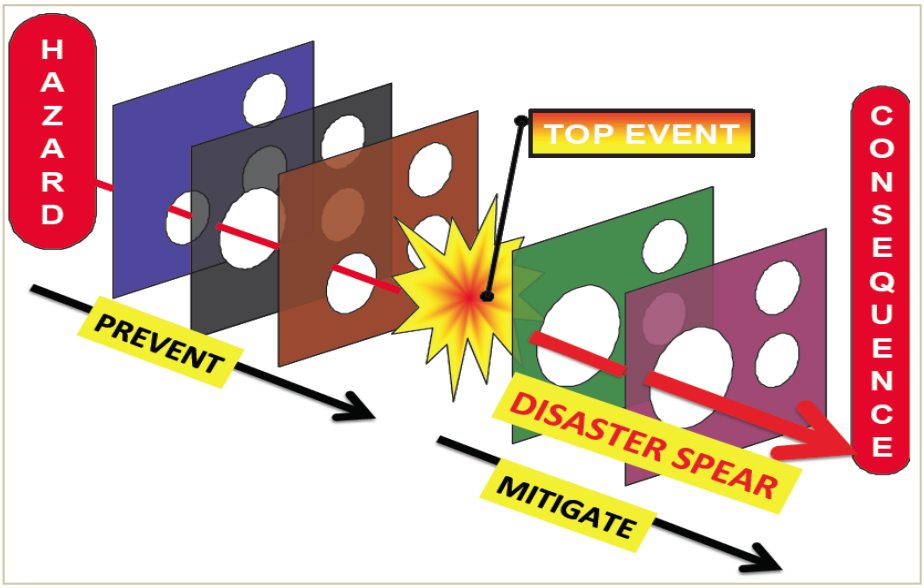

Figure 4: Defective prevention and mitigation barriers allow disaster spear penetration to cause major system disasters.

The numbers, sizes, and alignment of SRAM barrier holes are determined primarily by organizational management latent activities. The energy required for the disaster spear to penetrate the aligned barrier defects is provided by the system's responsible organizational management (i.e., systemic dysfunction in the management organization or its culture). Latent activities encompass lack of sufficient organizational management SRAM cognizance of or attention to major system accident risks, lack of commitment and capabilities to properly assess and manage major accident risks, dysfunctional safety cultures providing inadequate protection for production and long term costs and benefits, and absence of counting (providing valid and validated assessments of risks and short and long term costs and benefits).

The "top event" (sometimes referred to as the initiating event or failure event) is shown in Figure 4 as having barriers on both sides. Prevention barriers are important because they can identify major risks before they occur and thus allow an engineered system to adapt or cease operations in order to reduce risk and consequence levels to tolerable levels. For instance, leading SRAM indicators and a robust and dynamic risk assessment can alert management to the risk of an engineered system on an ongoing and current basis. Additionally, training and safety processes that are in place will act to reduce the human and system malfunction factors that can cause a major event.

When prevention barriers fail, it is a SRAM essential to have barriers in place that will counteract and control or mitigate the failure. These counter measures address aspects of vital importance in responding to the top event in an effective manner. For example, mitigation barrier considerations address the system's vulnerability to escalation from a loss of containment event and seek to harden the system's tolerance to such

[9] Process Safety Performance Indicators for the Refining and Petrochemical Industries, ANSI/API Recommended Practice RP-754, First Edition, April 2010, pp. 2, Figure 1.

events, such as increasing structural or thermal robustness by providing redundancy, resilience, and similar means of increased capacity to counter failure consequences. The mitigation barriers must be fit-for-purpose.

Implementation

Long-term (10+ years) studies of commercial – industrial organizations that have been successful and unsuccessful in development and maintenance of SRAM approaches and strategies that result in HRS have shown that "5 Cs" are needed to enable success:

- **Cognizance:** clear and continuous recognition of the threats and hazards that confront a system's abilities to realize acceptable performance and reliability (risk 'creep');
- **Capabilities:** organizations that have the shared knowledge, rules, skills, and other necessary resources to address all of the components that comprise a system during its life-cycle with particular emphasis on the "human" and "organizational" aspects;
- **Commitment:** top-down and bottom-up unwavering devotion of management, leadership, and follower-ship (teamwork) to a continuous program of improvement in the performance and reliability of the system;
- **Culture:** shared beliefs, attitudes, values, feelings, and resource allocation processes that bring into balance pressures of system Productivity and Protection thereby enabling realization of acceptable performance and reliability during the life of the system; and
- **Counting:** realistic quantitative analyses of system risks coupled with effective financial and social incentives (positive and negative) and metrics to encourage development and maintenance of systems that have ALARP risks.

The organizations that were not successful unintentionally developed defects or deficiencies in one or more of the "5 Cs." Success in implementation was only realized if *all* of the "5 Cs" were properly developed and maintained.

One of the most important of these "5 Cs" is Counting. Counting includes explicit up-front analyses of the "costs and benefits" associated with implementation of SRAM processes and procedures. Development and maintenance of effective SRAM processes and procedures cost substantial amounts of money and other important organizational resources. However, if the SRAM processes and procedures are effective, there are no (or vastly reduced numbers of) future major engineered system failures. There is a natural tension between "Production" (i.e., measured growth and profitability that are sensitive to costs) and "Protection" (resources invested to prevent failures – that do not happen – and that are difficult to "measure" until they happen). If this tension is not properly addressed, then experience has clearly demonstrated that organizations can expect to develop undesirable over-emphasis on engineered system Production (readily measured) and under-emphasis on engineered system Protection (not readily measured), with the attendant and undesirable consequence of major engineered system failures.

Robert Bea, PhD, PE (retired)
Professor Emeritus
Department of Civil & Environmental Engineering
University of California Berkeley